IN THE CLAIMS:

1 16.(new) A process for protecting a software product, sent from a server computer to a

2 computer, from unauthorized usage, the process comprising the steps of:

3 generating a first set of parameters from the computer before the software product

4 is sent to the computer,

5 sending the first set of parameters to the server computer before the software

6 product is sent to the computer,

7 creating, at the server computer, a single value from the first set of parameters be-

8 fore the software product is sent to the computer,

9 encrypting, at the server computer, the software product by using the single value

10 as the encryption key,

11 sending the encrypted software product to the computer,

12 encrypting, at the server computer, the single value by using members of the first

13 set of parameters as encryption keys,

14 sending the set of encrypted single values to the computer,

15 generating a second set of parameters from the computer,

16 decrypting members of the set of encrypted single values using members of the

17 second set of parameters as decryption keys, and

18 decrypting the encrypted software product by using the single value as the de-

19 cryption key.

1 17. (new) The process of claim 16 wherein the software product comprises data files

2 or streaming data.

1 18. (new) A process for protecting a software product, sent from a server computer to a

2 computer, from unauthorized usage, the process comprising the steps of:

3 generating a first set of parameters from the computer before the software product

4 is sent to the computer,

5 sending the first set of parameters to the server computer,

6 creating, at the server computer, a single value from the first set of parameters,

7 encrypting, at the server computer, the single value using members of the first set

8 of parameters as encryption keys,

9 sending the set of encrypted single values to the computer,

10 sending the software product to the computer,

11 generating a second set of parameters from the computer,

12 decrypting, at the computer, members of the set of encrypted single values by us-

13 ing members of the second set of parameters as decryption keys, and

14 authorizing access to the software product at the computer.

1 19. (new)   The process of claim 18 wherein the software product comprises data files

2 or streaming data.

1 20(new) The process of claim 18 further comprising the step wherein if the said decryp-

2 tion yields a number of identical single values, then

3 authorizing access to the software product at the computer.

1 21. (new) A process for protecting a software product, downloaded from a server com-

2 puter to a computer, from unauthorized usage, the process comprising the steps of:

3 encrypting, at the server computer, the software product using a first encryption

4 key created from a first set of data collected from the computer,

5 encrypting, at the server computer, the first encryption key by using the first set of

6 data as the encryption key,

7 downloading the encrypted first encryption key to the computer,

8 downloading the encrypted software product to the computer,

6

9   requesting access to the encrypted software product at the computer, and in re-

10   sponse thereto, generating a second set of data from the computer,

11   decrypting the encrypted first encryption key using the second set of data as the

12   decryption key,

13   decrypting the encrypted software product by using the resultant of said decryp-

14   tion of the encrypted first encryption key as the decryption key.

1   22. (new)   The process of claim 21 wherein the software product comprises data files

2   or streaming data.

1   23. (new) A process for protecting a software product, sent from a server computer to a

2   computer, from unauthorized usage, the process comprising the steps of:

3   encrypting, at the server computer, the software product before it has been sent to

4   the computer by using a first set of data collected from the computer as the encryption

5   key,

6   sending the encrypted software product to the computer,

7   requesting access to the encrypted software product at the computer, and in re-

8   sponse thereto, generating a second set of data from the computer, and

9   decrypting the encrypted software product by using the second set of data as the

10   decryption key.

1

2   24. (new)   The process of claim 23 wherein the software product comprises data files

3   or streaming data.

1   25. (new) A process for protecting a software product, sent from a server computer to a

2   computer, from unauthorized usage, the process comprising the steps of:

3   generating a first set of parameters from the computer before the software product

4   is sent to the computer,

5   sending the first set of parameters to the server computer,

6   creating, at the server computer, a single value from the first set of parameters,

7   encrypting, at the server computer, the single value by using members of the first

8   set of parameters as the encryption keys,

9   sending the set of encrypted single values to the computer,

10   sending the software product to the computer,

11   generating a second set of parameters from the computer,

12   decrypting members of the set of encrypted single values by using members of the

13   second set of parameters as the decryption keys, and

14   authorizing the execution of the software product on the computer.

1   26(new) The process of claims 25 further comprising the step wherein if the said de-

2   cryption yields a number of identical single values, then

3   authorizing the execution of the software product on the computer.

1   27. (new)   The process of claim 25 wherein the software product comprises data files

2   or streaming data.

1   28. (new) A process for protecting a software product from unauthorized usage by

2   authenticating a computer before the software product is downloaded from a server com-

3   puter to the computer, the process comprising the steps of:

4   executing a license agreement by a user for the software product, before the soft-

5   ware product is downloaded to the computer,

6   generating a first set of parameters from the computer before the software product

7   is downloaded to the computer,

8   sending the first set of parameters to the server computer before the software

9   product is downloaded to the computer,

10   generating a second set of parameters from the computer,

11   sending the second set of parameters to the server computer before the software

12 product is downloaded to the computer,

13   comparing, at the server computer, the first set of parameters to the second set of

14 parameters, and

15   starting the download of the software product to the computer

1 29. (new) The process of claim 28 wherein the software product comprises data files

2 or streaming data.

1 30. (new) The continuing process of claim 28 further comprising the steps of: if the said

2 download fails or is paused,

3   generating a third set of parameters from the computer,

4   sending the third set of parameters to the server computer,

5   comparing, at the server computer, the third set of parameters with the first or

6 second set of parameters stored at the server, and

7   resuming the download of the software product to the computer.

1 31. (new) The process of protecting a software product from unauthorized usage, sent

2 from a sever computer to a computer, the process comprising the steps of:

3   generating a set of data from the computer before the software product is sent to

4 the computer,

5   sending the set of data to the server computer before the software product is sent

6 to the computer,

7   encrypting, at the server computer, the software product by using an encryption

8 key created from the set of data,

9   sending the encrypted software product to the computer,

10   generating a second set of data from the computer, and

11   decrypting the encrypted software product by using a decryption key created from

12 the second set of data.

1   32. (new)   The process of claim 31 wherein the software product comprises data files

2   or streaming data.

1   33. (new) The process of protecting a software product from unauthorized usage, the

2   software product downloaded from a server computer to a first computer and moved to a

3   second computer, comprising the steps of:

4   executing a license agreement by a user for the software product before the soft-

5   ware product is sent to the first computer,

6   generating a set of parameters on the first computer before the software product is

7   sent to the first computer,

8   sending the set of parameters to the server computer,

9   downloading the software product to the first computer,

10   executing software product on the first computer,

11   moving said software product to a second computer,

12   requesting access to the software product, and in response thereto, generating a set

13   of parameters from the second computer, and

14   not authorizing the execution of the software product on the second computer.

1   34. (new)   The process of claim 33 wherein the software product comprises data files

2   or streaming data.

1   35. (new) The continuing process of claim 33 further comprising the step of:

2   displaying a message to the user.

1   36. (new) The continuing process of claim 33 further comprising the step of:

2   automatically notifying the vendor